

Structure theorem of unitary design

Yuan Li

Abstract

An (n, k) unitary design is an n by n matrix \mathcal{U} , where each entry is a complex linear combination of $z_i, z_i^*, i = 1, \dots, k$, such that $\mathcal{U}^H \mathcal{U} = (|z_1|^2 + \dots + |z_k|^2) I_n$. Based on the work of Tirkkonen and Hottinen, which first proved a $\frac{\lceil \log_2 n \rceil + 1}{2^{\lceil \log_2 n \rceil}}$ upper bound of k/n by making a crucial observation between unitary design and group representation, we prove the structure theorem of unitary design.

1 Background and Related Work

Complex orthogonal design \mathcal{O} with parameter (p, n, k) is a $p \times n$ matrix where each entry is a complex linear combination of z_1, \dots, z_k such that $\mathcal{O}^H \mathcal{O} = (|z_1|^2 + \dots + |z_k|^2) I_n$. Generally, we are interested two kinds of problems:

- (Parameter) For what p, n, k , there exists a (p, n, k) complex orthogonal design?
- (Structure) What is the structure of (p, n, k) complex orthogonal design?

An (n, k) unitary design is an (n, n, k) complex orthogonal design, which is also called square complex orthogonal design.

For unitary design, Tirkkonen and Hottinen [11] proved an upper bound $\frac{\lceil \log_2 n \rceil + 1}{2^{\lceil \log_2 n \rceil}}$ of k/n by making a crucial connection between unitary design and group representation (Clifford algebra). In fact, following their observation, the structure of unitary design could be clarified, which is what we did in this paper. In [13], Liang proved that (n, k) unitary design, $n = 2^a(2b + 1)$, exists if and only if $k \leq a + 1$, which follows from an observation that an (n, k) unitary design induces a family of $2k$ matrices in $GL_n(\mathbb{C})$ such that all nonzero linear combinations are nonsingular. It is known that the size of such family of matrices is bounded by $2a + 2$, which is a highly nontrivial result proved by J. F. Adams, Lax and Phillips in [1], [2], [3].

For complex orthogonal design, both the parameter and the structure problem are wide open, and little is known except some restricted cases. In [22], Wang and Xia proved that $k/p \leq 3/4$. In [13], when linear combination is not allowed, i.e., each entry is $\pm z_i, \pm z_i^*$ or 0, Liang proved a tight upper bound $\frac{m}{2m+1}$ of k/p , where $m = \lceil \frac{n}{2} \rceil$. In [6], [7], S. S. Adams, Karst, Murgugan, and Pollack proved a tight upper bound of p when k/p reaches the maximal for CODs without linear combinations. By putting a further restriction that submatrices $\begin{pmatrix} \pm z_j & 0 \\ 0 & \pm z_j^* \end{pmatrix}$ and $\begin{pmatrix} \pm z_j^* & 0 \\ 0 & \pm z_j \end{pmatrix}$ are forbidden, Li and Kan solved both the parameter and structure problem [14].

The aforementioned investigation of COD is motivated by space-time block codes in wireless communication systems with multiple transmit and receive antennas. Since the pioneering work by Alamouti [8] in 1998, and the work by Tarokh et al. [19], [20], complex orthogonal designs have become an effective technique for the design of space-time block codes (STBC). Because of its applications in space-time block codes, quite a lot of constructions have been proposed [4], [9], [12], [14], [13], [15], [17], [18], [21].

In this paper, we solve the structure theorem of unitary design, which says every (n, k) unitary design is equivalent to some simple canonical form, thus classifies all (n, k) unitary designs into $\frac{n}{2^{k-1}}$ different classes.

2 Main Result

Definition 1. An (n, k) unitary design is an $n \times n$ matrix \mathcal{U} , where each entry is a complex linear combination of z_i, z_i^* , $i = 1, \dots, k$, such that

$$\mathcal{U}^H \mathcal{U} = (|z_1|^2 + \dots + |z_k|^2) I_n.$$

Assuming \mathcal{U} is an (n, k) unitary design, and $V, W \in U_n$, then $V\mathcal{U}W$ is also an (n, k) unitary design. Because

$$\begin{aligned} (V\mathcal{U}W)^H (V\mathcal{U}W) &= W^H \mathcal{U}^H V^H V \mathcal{U} W \\ &= W^H \mathcal{U}^H \mathcal{U} W \\ &= W^H (|z_1|^2 + \dots + |z_k|^2) I_n W \\ &= (|z_1|^2 + \dots + |z_k|^2) I_n. \end{aligned}$$

We say unitary designs \mathcal{U} and $V\mathcal{U}W$ are equivalent, which defines an equivalence relation.

Before stating our main result, we need to define a set of canonical unitary designs. Let

$$\mathcal{C}_1 = (z_1)$$

For $k > 1$, let

$$\mathcal{C}_k = \begin{pmatrix} \mathcal{C}_{k-1} & z_k I_{2^{k-1}} \\ -z_k^* I_{2^{k-1}} & \mathcal{C}_{k-1}^H \end{pmatrix}.$$

And define \mathcal{C}_k^- by replacing z_k by z_k^* in \mathcal{C}_k .

Let's verify \mathcal{C}_k and \mathcal{C}_k^- are unitary designs by induction. Since $|z_k|^2 = |z_k^*|^2$, it's sufficient to prove \mathcal{C}_k is unitary design. When $k = 1$, it's obvious. Assuming \mathcal{C}_{k-1} is a unitary design, let's verify \mathcal{C}_k .

$$\begin{aligned} \mathcal{C}_k^H \mathcal{C}_k &= \begin{pmatrix} \mathcal{C}_{k-1} & z_k I_{2^{k-1}} \\ -z_k^* I_{2^{k-1}} & \mathcal{C}_{k-1}^H \end{pmatrix}^H \begin{pmatrix} \mathcal{C}_{k-1} & z_k I_{2^{k-1}} \\ -z_k^* I_{2^{k-1}} & \mathcal{C}_{k-1}^H \end{pmatrix} \\ &= \begin{pmatrix} \mathcal{C}_{k-1}^H \mathcal{C}_{k-1} + |z_k|^2 I_{2^{k-2}} & 0 \\ 0 & \mathcal{C}_{k-1}^H \mathcal{C}_{k-1} + |z_k|^2 I_{2^{k-2}} \end{pmatrix} \\ &= \begin{pmatrix} (|z_1|^2 + \dots + |z_k|^2) I_{2^{k-2}} & 0 \\ 0 & (|z_1|^2 + \dots + |z_k|^2) I_{2^{k-2}} \end{pmatrix} \\ &= (|z_1|^2 + \dots + |z_k|^2) I_{2^{k-1}}, \end{aligned}$$

where the last second step is by induction hypothesis that $\mathcal{C}_{k-1}^H \mathcal{C}_{k-1} = (|z_1|^2 + \dots + |z_{k-1}|^2)I_{2^{k-2}}$.

Now we are ready to state our main result, which is a structure theorem of unitary design.

Theorem 2. *An (n, k) unitary design \mathcal{U} exists if and only if*

$$k \leq a + 1,$$

where $n = 2^a(2b + 1)$, and there exists $V, W \in U_n$ such that

$$\begin{aligned} \mathcal{U} &= V \text{diag}(\mathcal{C}_k^\pm, \mathcal{C}_k^\pm, \dots, \mathcal{C}_k^\pm) W \\ &= V \left(\bigoplus_{i=1}^{n/2^{k-1}} \mathcal{C}_k^\pm \right) W, \end{aligned}$$

where \mathcal{C}_k^\pm denotes either \mathcal{C}_k or \mathcal{C}_k^- .

Before starting to prove, let's briefly sketch the overall idea. First, the existence of an unitary design implies the existence of a set of matrices $E_1, \dots, E_{2k} \in U_n$ such that, for any $i \neq j$,

$$E_i^H E_j + E_j^H E_i = 0. \quad (1)$$

Then following a crucial step made in [11], define $G_i = E_0^H E_i$, which is also unitary, then (1) becomes

$$G_i G_j = -G_j G_i \quad (2)$$

for all $i \neq j$, and $G_i^2 = -1$ for all $i \in \{2, \dots, 2k\}$. If we view g_2, \dots, g_{2k} as a set of generators of a group satisfying relations $g_i^2 = -1$ and $g_i g_j = -g_j g_i$, then matrices G_2, \dots, G_{2k} is a linear representation of the group. In fact, this is the defining relation of generators of Clifford algebra, which has been well studied in mathematics. By some classical results on the representations of finite group, it turns out that this group has only two nondegenerate irreducible representations, which are induced by exactly \mathcal{C}_k^\pm . Since any linear representation of finite group can be decomposed into a direct sum of irreducible ones, we obtain our structure theorem.

Let's start our proof formally. Given an (n, k) unitary design \mathcal{U} , writing $z_i = x_i + \sqrt{-1}y_i$, $x_i, y_i \in \mathbb{R}$, expand \mathcal{U} as follows.

$$\begin{aligned} \mathcal{U} &= \sum_{i=1}^k (z_i A_i + z_i^* B_i) \\ &= \sum_{i=1}^k ((x_i + \sqrt{-1}y_i)A_i + (x_i - \sqrt{-1}y_i)B_i) \\ &= \sum_{i=1}^k x_i (A_i + B_i) + \sum_{i=1}^k y_i \sqrt{-1} (A_i - B_i). \end{aligned}$$

For convenience, let $E_i = A_i + B_i$, $E_{i+k} = \sqrt{-1}(A_i - B_i)$ and $x_{k+i} = x_i$. Then,

$$\mathcal{U} = \sum_{i=1}^{2k} x_i E_i. \quad (3)$$

By taking $x_i = 1$ and all others 0, from condition $\mathcal{U}^H \mathcal{U} = (|z_1|^2 + \dots + |z_k|^2)I_n$, we have

$$E_i^H E_i = I_n. \quad (4)$$

By taking $x_i = x_j = 1$ and all others 0, we have

$$E_i^H E_j + E_j^H E_i = 0. \quad (5)$$

On the other hand, if (4) and (5) are satisfied,

$$\begin{aligned} \mathcal{U}^H \mathcal{U} &= \left(\sum_{i=1}^{2k} x_i E_i \right)^H \left(\sum_{i=1}^{2k} x_i E_i \right) \\ &= \sum_{i=1}^{2k} x_i^2 E_i^H E_i + \sum_{1 \leq i < j \leq 2k} x_i x_j (E_i^H E_j + E_j^H E_i) \\ &= \left(\sum_{i=1}^{2k} x_i^2 \right) I_n, \end{aligned}$$

which means (4) and (5) are both necessary and sufficient. So, we have the following proposition.

Proposition 3. *An (n, k) unitary design exists if and only if there exists matrices $E_1, \dots, E_{2k} \in U_n$, such that*

$$E_i^H E_j + E_j^H E_i = 0$$

for all $1 \leq i \neq j \leq 2k$.

For convenience of description, let's left shift the indices of E_i and x_i by 1. Let's define $G_i = E_0^H E_i$. Then $G_i^H G_i = (E_0^H E_i)^H (E_0^H E_i) = E_i^H E_0 E_0^H E_i = I_n$, which means G_i is also unitary. Further, G_i is anti-Hermitian, whence

$$G_i^H = ((E_0)^H E_i)^H = E_i^H E_0 = -E_0^H E_i = -G_i,$$

where the last second step is from $E_0^H E_i + E_i^H E_0 = 0$. Further, we have

$$\begin{aligned} G_i G_j &= -G_i^H G_j \\ &= -(E_0^H E_i)^H (E_0^H E_j) = -E_i^H E_0 E_0^H E_j \\ &= -E_i^H E_j = E_j^H E_i = E_j^H E_0 E_0^H E_i \\ &= (E_0^H E_j)^H (E_0^H E_i) = G_j^H G_i \\ &= -G_j G_i, \end{aligned}$$

which means G_i and G_j are anti-commuting.

Now, let's artificially define a group \mathcal{G}_{2k-1} generated by g_1, \dots, g_{2k-1} satisfying $g_i^2 = -1$ and $g_i g_j = -g_j g_i$. Notice that 1 and -1 are simply two elements in the group, where 1 is the identity, and $g_i, -g_i$ are two different elements satisfying $-g_i = (-1)g_i$. Formally, the group consists of the following elements

$$\{\pm \prod_{i \in S} g_i : S \subseteq \{1, \dots, 2k-1\}\}.$$

Thus, the size of the group \mathcal{G}_{2k-1} is 2^{2k} .

Lemma 4 and Lemma 5 are about the irreducible representations of the group \mathcal{G}_{2k-1} , which are proved in [11], and we reproduce the proof here for completeness.

Lemma 4. *For group \mathcal{G}_{2k-1} , if ρ is an irreducible representation with $\dim > 1$, then ρ' defined by $\rho'(g_i) = \rho(g_i)$ for all $i \neq 1$, and $\rho'(g_1) = -\rho(g_1)$ is another 2^{k-1} dimensional irreducible representation.*

Proof. First, notice that $\prod_{i=1}^{2k-1} g_i$ is a central element of the group. Because for any $S \subseteq \{1, \dots, 2k-1\}$, where $S = \{s_1, \dots, s_l\}$,

$$\begin{aligned} \left(\prod_{i=1}^{2k-1} g_i \right) \left(\prod_{i \in S} g_i \right) &= (-1)^{2k-2} g_{s_1} \left(\prod_{i=1}^{2k-1} g_i \right) \left(\prod_{i \in S \setminus \{s_1\}} g_i \right) \\ &= g_{s_1} g_{s_2} \left(\prod_{i=1}^{2k-1} g_i \right) \left(\prod_{i \in S \setminus \{s_1, s_2\}} g_i \right) \\ &= \left(\prod_{i \in S} g_i \right) \left(\prod_{i=1}^{2k-1} g_i \right). \end{aligned}$$

By Schur's lemma, since ρ is irreducible, $\rho(\prod_{i=1}^{2k-1} g_i) = \lambda I_n$, where $\lambda \in \mathbb{C}$, which implies

$$\rho(g_2 \dots g_{2k-1}) = \rho(-g_1^2) \rho(g_2 \dots g_{2k-1}) = \rho(-g_1) \rho(g_1 \dots g_{2k-1}) = -\rho(g_1) \lambda I_n,$$

i.e.,

$$\rho(g_1) = -\frac{1}{\lambda} \rho(g_2 \dots g_{2k-1}). \quad (6)$$

Assume to the contrary that there exists a similarity transformation $T \in GL_n(\mathbb{C})$ such that $\rho' = T^{-1} \rho T$. By the definition of ρ' , we have

$$\rho(g_i) = T^{-1} \rho(g_i) T$$

for all $i = 2, \dots, 2k-1$. And

$$\begin{aligned} \rho'(g_1) &= T^{-1} \rho(g_1) T \\ &= T^{-1} \left(-\frac{1}{\lambda} \rho(g_2) \rho(g_3) \dots \rho(g_{2k-1}) \right) T \\ &= -\frac{1}{\lambda} (T^{-1} \rho(g_2) T) (T^{-1} \rho(g_3) T) \dots (T^{-1} \rho(g_{2k-1}) T) \\ &= -\frac{1}{\lambda} \rho(g_2) \dots \rho(g_{2k-1}) \\ &= \rho(g_1), \end{aligned}$$

which is a contradiction! \square

Next lemma shows that there are only two nondependence irreducible representations of \mathcal{G}_{2k-1} , and both of them are of dimension 2^{k-1} .

Lemma 5. *Group \mathcal{G}_{2k-1} has $2^{2k-1} + 2$ irreducible representations. Two are 2^{k-1} dimensional, 2^{2k-1} are 1-dimensional.*

Proof. First, let's construct 2^{2k-1} nonequivalent one-dim representations. For any $J \subseteq \{1, \dots, 2k-1\}$, let $\rho(1) = \rho(-1) = 1$, $\rho(g_i) = 1$ if $i \notin J$ and $\rho(g_j) = -1$. It's easy to see ρ is a representation of \mathcal{G}_{2k-1} , and they are nonequivalent.

Then, apply the counting formula, e.g. section 2.4 in [16],

$$|\mathcal{G}_{2k-1}| = \sum_{i=1}^l n_i^2,$$

where n_i is the dimension of each irreducible representations, and l equals the number of conjugacy classes. We claim $l = 2^{2k-1} + 2$, which will be proved at the end of this proof. By the existence of 2^{2k-1} one-dim representations, and Lemma 4, we have

$$2n_1^2 = 2^{2k-1},$$

which implies $n_1 = 2^{k-1}$, i.e., there exist two irreducible two representations with dimension 2^{k-1} .

Finally, we need to prove our claim: there are $2^{2k-1} + 2$ conjugacy classes. If an element commute with all elements, then itself forms a conjugacy class; otherwise, itself and its negation forms a conjugacy class. For $\pm 1, \pm \prod_{i=1}^{2k-1} g_i$, they belong to the former case; for any $\emptyset \neq S \subsetneq [2k-1]$, with $S = \{s_1, \dots, s_m\}$, there exists $s'_m \notin S$, it's easy to verify $\pm \prod_{i \in S} g_i$ is anti-commuting with $(\prod_{i=1}^{m-1} s_i) s'_m$. Therefore, there are $2^{2k-1} + 2$ conjugacy classes, which completes our proof. \square

In fact, we can write down all the irreducible representations explicitly, for example, see [11]. However, we could avoid doing that.

Lemma 6. *Unitary designs \mathcal{C}_k and \mathcal{C}_k^- induces two nonequivalent 2^{k-1} dimensional irreducible representations.*

Proof. Denote by ρ and ρ' the group representations induced by \mathcal{C}_k and \mathcal{C}_k^- . Since $\dim \rho = 2^{k-1}$, by Lemma 5, ρ is either irreducible or a direct sum of 2^{k-1} one-dim representations. Since all one-dim representation is degenerate, and ρ is non-degenerate, it should be a 2^{k-1} dimensional irreducible representation, as well as ρ' .

As usual, let $\mathcal{C}_k = \sum_{i=1}^k (z_i A_i + z_i^* B_i)$, and then $E_i = A_i + B_i$, $E_{i+k} = \sqrt{-1}(A_i - B_i)$. The only difference between \mathcal{C}_k and \mathcal{C}_k^- is that z_k is conjugated, which results in swapping A_k and B_k , and thus E_{2k} is negated while all the other E_i 's are unchanged, i.e., only G_{2k-1} is negated. By Lemma 4, we know that ρ' is another irreducible representation different from ρ . \square

Before proving the structure theorem, let's prove a lemma about unitary representations of a finite group, which says if two unitary representations are similar, then they are unitarily similar, in the sense that the linear transformation is unitary. We feel that this result is very likely to be known in math literature.

Lemma 7. *Let $\pi, \sigma : G \rightarrow U_n(\mathbb{C})$ be two unitary representations of finite group G . If π, σ are equivalent, i.e., there exists $T \in GL_n(\mathbb{C})$ such that*

$$T\pi(g) = \sigma(g)T, \quad \forall g \in G,$$

then π and σ unitarily equivalent, that is, there exists $T' \in U_n$ such that

$$T'\pi(g) = \sigma(g)T', \quad \forall g \in G.$$

Proof. Prove by construction. Since $T\pi = \sigma T$ and π is unitary, which implies $\pi(g)^* = \pi(g^{-1})$, we have $\pi T^* = (\pi^{-1})^* T^* = (T\pi^{-1})^* = (\sigma^{-1}T)^* = T^*(\sigma^{-1})^* = T^*\sigma$. Thus, T^* also intertwines with π and σ . Define $|T| = \sqrt{T^*T}$, which is meaningful since a positive-semidefinite Hermitian matrix has a unique positive-semidefinite square root.

Letting $T' = T|T|^{-1}$, we claim this is the desired T' . First, let's verify that T' is unitary.

$$\begin{aligned} T'T' &= (T|T|^{-1})^* T|T|^{-1} \\ &= |T|^{-1} T^* T |T|^{-1} = |T|^{-1} |T|^2 |T|^{-1} = I. \end{aligned}$$

Then, let's verify T' intertwines, i.e., $T'\pi = \sigma T'$, which is $T|T|^{-1}\pi = \sigma T|T|^{-1} = T\pi|T|^{-1}$. Since T is invertible, it suffices to prove $|T|^{-1}\pi = \pi|T|^{-1}$, that is, $|T|$ commutes with π . Notice that T^*T commutes with π , since $T^*T\pi = T^*\sigma T = \pi T^*T$, and $|T|$ can be approximated by polynomials in T^*T (For example, expand the square root in Taylor series). Combining with the fact that every polynomial in T^*T commutes with π , we have $|T|$ also commutes with π , which completes our proof. \square

Now, we are ready to prove the structure theorem of unitary designs.

Proof. Let \mathcal{U} be an (n, k) unitary design. As in (3), splitting the real part and imaginary part, write

$$\mathcal{U} = x_1 E_1 + x_2 E_2 + \dots + x_{2k} E_{2k}.$$

As usual, let $E_i = E_{i+1}$, $i = 0, \dots, 2k-1$, and $G_i = E_0^H E_i$ for $i = 1, 2, \dots, 2k-1$. It turns out G_1, \dots, G_{2k-1} induce a representation ρ , which is a unitary, nondegenerate representation of group \mathcal{G}_{2k-1} .

Since every representation of a finite group is a direct sum of irreducible ones, e.g., section 1.4 in [16], there exists $T \in GL_n(\mathbb{C})$ such that

$$\begin{aligned} G_i &= T^{-1} \rho_1(g_i) \oplus \dots \oplus \rho_m(g_i) T \\ &= T^{-1} \begin{pmatrix} \rho_1(g_i) & & & \\ & \rho_2(g_i) & & \\ & & \ddots & \\ & & & \rho_m(g_i) \end{pmatrix} T, \end{aligned} \quad (7)$$

where ρ_1, \dots, ρ_m are irreducible representations of group \mathcal{G}_{2k-1} . By Lemma 7, T could be chosen to be unitary.

Next, we shall show that ρ_1, \dots, ρ_m are all nondegenerate. Otherwise, assume ρ_1 is degenerate without loss of generality, i.e., $\rho_1(1) = \rho_1(-1)$. Then,

$$\rho(g_1) = G_1 = T^{-1} \begin{pmatrix} \rho_1(1) & & & \\ & \rho_2(1) & & \\ & & \ddots & \\ & & & \rho_m(1)T \end{pmatrix}$$

and

$$\rho(-g_1) = -G_1 = T^{-1} \begin{pmatrix} \rho_1(-1) = \rho_1(1) & & & \\ & \rho_2(-1) & & \\ & & \ddots & \\ & & & \rho_m(-1)T \end{pmatrix}.$$

Thus

$$\begin{pmatrix} \rho_1(1) & & & \\ & \rho_2(1) & & \\ & & \ddots & \\ & & & \rho_m(1) \end{pmatrix} = \begin{pmatrix} -\rho_1(1) & & & \\ & -\rho_2(-1) & & \\ & & \ddots & \\ & & & -\rho_m(-1) \end{pmatrix},$$

which implies $\rho_1(1) = -\rho_1(1) \Rightarrow \rho_1 = 0$. Contradiction!

By Lemma 5, all non-degenerate irreducible representations are of dimension 2^{k-1} , we have $\dim(\rho_i) = 2^{k-1}$ for $i = 1, \dots, m$, which implies $n = m2^{k-1}$, i.e., $2^a(2b+1) = m2^{k-1} \Rightarrow k \leq a+1$, which proves the first part of the theorem.

In order to prove the second part, what we do next is to expand \mathcal{U} by (7). By definition, $G_i = E_0^H E_i \Rightarrow E_i = E_0 G_i$. By (7),

$$E_i = E_0 T^{-1} \begin{pmatrix} \rho_1(g_i) & & & \\ & \rho_2(g_i) & & \\ & & \ddots & \\ & & & \rho_m(g_i) \end{pmatrix} T.$$

Then,

$$\begin{aligned} \mathcal{U} &= x_0 E_0 + x_1 E_1 + \dots + x_{2k-1} E_{2k-1} \\ &= x_0 E_0 + \sum_{i=1}^{2k-1} x_i E_0 T^{-1} \begin{pmatrix} \rho_1(g_i) & & & \\ & \rho_2(g_i) & & \\ & & \ddots & \\ & & & \rho_m(g_i) \end{pmatrix} T \\ &= E_0 T^{-1} (I x_0) T + E_0 T^{-1} \begin{pmatrix} \sum_{i=1}^{2k-1} x_i \rho_1(g_i) & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \sum_{i=1}^{2k-1} x_i \rho_m(g_i) \end{pmatrix} T \\ &= E_0 T^{-1} \begin{pmatrix} x_0 I + \sum_{i=1}^{2k-1} x_i \rho_1(g_i) & & & \\ & \ddots & & \\ & & \ddots & \\ & & & x_0 I + \sum_{i=1}^{2k-1} x_i \rho_m(g_i) \end{pmatrix} T \\ &= E_0 T^{-1} \begin{pmatrix} \mathcal{C}_k^\pm & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \mathcal{C}_k^\pm \end{pmatrix} T. \end{aligned}$$

Setting $V = E_0 T^{-1}$ and $W = T$, the second part of theorem is proved. \square

Now, both the parameter and the structure problem of unitary design (square complex orthogonal design) are solved. For further research, it's tempting to apply the group representation approach for the nonsquare complex orthogonal if possible.

Acknowledgement

We would like to thank Mateusz Wasilewski for giving the proof of Lemma 7 on MathOverflow.

References

- [1] J. F. Adams, “*Vector fields on spheres*,” Ann. Math., vol. 75, no. 2, pp. 603-632, 1962.
- [2] J. F. Adams, P. D. Lax, and R. S. Phillips, “*On matrices whose real linear combinations are nonsingular*,” in Proc. Amer. Math. Soc., vol. 16, 1965, pp. 318-322.
- [3] J. F. Adams, P. D. Lax, and R. S. Phillips, “*Corrections to On matrices whose real linear combinations are nonsingular*,” in Proc. Amer. Math. Soc., vol. 17, 1966, pp. 945-947.
- [4] S. S. Adams, J. Davis, N. Karst, M. K. Murugan, B. Lee, M. Crawford, C. Greeley, “*Novel classes of minimal delay and low PAPR rate 1/2 complex orthogonal designs*,” IEEE Trans. Inf. Theory, vol. 57, no. 4, pp. 2254-2262, Apr. 2011.
- [5] S. S. Adams, N. Karst, M. K. Murugan and T. A. Wysocki, “*On transceiver signal linearization and the decoding delay of maximum rate complex orthogonal space-time block codes*,” IEEE Trans. Inf. Theory, vol. 57, no. 6, pp. 3618-3621, Jun. 2011.
- [6] S. S. Adams, N. Karst, and J. Pollack, “*The minimum decoding delay of maximum rate complex orthogonal space-time block codes*,” IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2677-2684, Aug. 2007.
- [7] S. S. Adams, N. Karst, M. K. Murugan., “*The final case of the decoding delay problem for maximum rate complex orthogonal designs*,” IEEE Trans. Inf. Theory, vol. 56, no. 1, pp. 103-122, Jan. 2010.
- [8] S. Alamouti, “*A simple transmit diversity technique for wireless communications*,” IEEE J. Select. Areas Commun., vol. 16, pp. 1451-1458, Oct. 1998.
- [9] S. Das and B. S. Rajan, “*Low-delay, high-rate nonsquare complex orthogonal designs*,” IEEE Trans. on Information Theory, vol. 58, no. 5, pp. 2633-2647, May, 2012.
- [10] A. V. Geramite and N. J. Pullman, “*Orthogonal Designs: Quadratic Forms and Hadamard Matrices (Lecture Notes in Pure and Applied Mathematics)*,” New York: Marcel Dekker, vol. 43, 1979.
- [11] O. Tirkkonen, and A. Hottinen, “*Square-matrix embeddable space-time block codes for complex signal constellations*,” IEEE Trans. on Information Theory, vol. 48, no. 2, Feb. 2002.
- [12] H. Kan and H. Shen, “*A counterexample for the open problem on the minimal delays of orthogonal designs with maximal rates*,” IEEE Trans. Inf. Theory, vol. 51, no. 1, pp. 355-359, Jan. 2005.
- [13] X-B. Liang, “*Orthogonal designs with maximal rates*,” IEEE Trans. Inf. Theory, vol. 49, no. 10, pp. 2468-2503, Oct. 2003.

- [14] Yuan Li and Haibin Kan, “Complex orthogonal designs with forbidden 2×2 submatrices”, IEEE Trans. on Information Theory, vol. 58, no. 7, pp. 4825–4836, July, 2012.
- [15] K. Lu, S. Fu, and X. G. Xia, “Closed-form designs of complex orthogonal space-time block codes of rates $(k+1)/(2k)$ for $2k-1$ or $2k$ transmit antennas,” IEEE Trans. Inf. Theory, vol. 51, no. 12, pp. 4340-4347, Dec. 2005.
- [16] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, 2008.
- [17] W. Su, X.-G. Xia, and K. J. R. Lui, “A systematic design of high-rate complex orthogonal space-time block codes,” IEEE Commun. Lett. vol. 8, no. 6, pp. 380-382, Jun. 2004.
- [18] J. Seberry, S. A. Spence, and T. A. Wysocki, “A construction technique for generalized complex orthogonal designs and applications to wireless communications,” Linear Algebra and its Applications 405 (2005) 163-167.
- [19] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, “Space-time block codes from orthogonal designs,” IEEE Trans. Inf. Theory, vol. 45, no. 5, pp. 1456-1467, July 1999.
- [20] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, “Correction to ‘Space-time block codes from orthogonal designs,’” IEEE Trans. Inf. Theory, vol. 46, no. 1, Jan. 2000.
- [21] L. C. Tran, T. A. Wysocki, J. Seberry, A. Mertins and S. S. Adams, “Novel constructions of improved square complex orthogonal designs for eight transmit antennas,” IEEE Trans. Inf. Theory, vol. 55, no. 10, Oct. 2009.
- [22] H. Wang and X-G. Xia, “Upper bounds of rates of complex orthogonal space-time block codes,” IEEE Trans. Inf. Theory, vol. 49, no. 10, pp. 2788-2796, Oct. 2003.